38. (Amended) A system for generating a security policy for a network, said network including a plurality of hosts, said system comprising:

a memory for storing computer-readable code; and

a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network;

receive an assignment of roles to said hosts in said network; and

generate said security policy from said received definitions and assignments.

REMARKS

This Amendment is submitted in response to the outstanding Office Action, dated February 27, 2002. Claims 1 through 38 are presently pending in the above-identified patent application. Claims 9-28, 36 and 37 have been withdrawn from consideration, without prejudice. Claims 1, 29, 35 and 38 have been amended. No additional fee is due.

In the Office Action, the Examiner required an election of claims between Group I, II and Group III. In addition, the Examiner rejected Claim 29 under 35 U.S.C. §102(e) as being anticipated by Reid et al. (United States Patent Number 6,182,226). The Examiner rejected Claims 1-8, 19-28, 30-35 and 38 under 35 U.S.C. §103(a) as being unpatentable over Reid et al. in view of Grennan, "Firewalling and Proxy Server HOWTO," Nov. 1996.

The present invention is directed to a firewall manager that generates a security policy for a particular network environment, and automatically generates the firewall-specific configuration files from the security policy simultaneously for multiple gateways. A model compiler translates an entity-relationship model into the appropriate firewall configuration files. The security policy is expressed in terms of "roles," which are used to define network capabilities of sending and receiving services. Roles capture the *topology-independent* and firewall-independent essence of a policy. *A role is a property that may be assumed by different hosts in the network.* A group of roles may be collectively assigned as role-groups. Host-groups or individual hosts are the entities to which role-groups are attached (via the attribute assumed-roles) and thus this is the place where the security policy (modeled by roles and role-groups) is linked to the network topology.

The Examiner required an election of claims between the claims of Group I and Group II. Group I includes claims 1-8, 29-35 and 38, drawn to generating a security policy/rules that determine or define the ability of a host to send and receive packets. Group II includes claims 9-17 and 18-28, drawn to utilizing a model topology/definition language to produce an entity relationship model. Applicants hereby affirm the election of the claims of Group I, and withdraw the claims of Group II from consideration, without prejudice.

The Examiner rejected Claim 29 under 35 U.S.C. §102(e) as being anticipated by Reid et al. (United States Patent Number 6,182,226). The Examiner asserts that Reid et al. discloses restricting the communication of packets to and from network interfaces using a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface is assigned. The Examiner further asserts that the firewall comprises a plurality of regions (assignment of roles) having policies (rules) configured (generated) for each of the regions. Citing col. 2, lines 8-17. The Examiner notes that Reid et al. disclose various commands for setting up access control rules that are applied to the regions (assignment of roles) in column 11.

Reid et al. is directed to a system and method for grouping networks by network region to enforce a security policy. As recognized by the Examiner, Reid et al. disclose a "firewall comprising a plurality of regions, wherein a set of policies have been configured for each of the plurality of regions; *wherein each of the plurality of network interfaces is assigned to only one of the plurality of regions*; wherein at least one of the plurality of network interfaces is assigned to a particular region; and wherein communication to and from each of the plurality of network interfaces is restricted in accordance with the set of policies configured for the one of the plurality of regions to which the one of the plurality of network interfaces has been assigned." Col. 2, lines 8-17 (emphasis added).

In the rejection, the Examiner has equated the term "region" from Reid et al. with the term "roles" as recited in the claims of the present application. In the network environment of Reid et al., each of the machines (hosts) are identified by a fixed IP address and are physically connected to a given network (through a network interface). A firewall provides physical separation among each of the different networks or sub-networks and thereby creates "regions." A "region" is thus a collection of the IP addresses of a corresponding network. Each network interface is assigned to exactly one region. See, col. 2, lines 10-11. *The network interface to which a machine is connected determines the "region" to which the machine belongs.* The "regions" of Reid et al. are thus clearly network-topology

dependent and cannot be "assigned to said hosts independently of a topology of said network," as required by each of the independent claims, as amended.

The Examiner rejected Claims 1-8, 19-28, 30-35 and 38 under 35 U.S.C. §103(a) as being unpatentable over Reid et al. in view of Grennan, "Firewalling and Proxy Server HOWTO," Nov. 1996. Grennan was cited by the Examiner for its teaching of the generation of a configuration file for a firewall. (citing section 4.2). Grennan discloses the generation of a configuration file for a *specific* firewall. In any case, Grennan does not disclose or suggest "receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network," as required by each of the independent claims, as amended. Support for the amendments are found, for example, at page 6, lines 13-14.

Claims 2 through 8 and 30 through 34 are dependent on Claims 1 or 29 and are therefore patentably distinguished over Reid et al. and Grennan, alone or in combination, because of their dependency from independent Claims 1 or 29 for the reasons set forth above, as well as other elements these claims adds in combination to their base claim. For example, claim 3 specifies that a security policy for said network is "expressed in terms of said roles defining network capabilities of sending and receiving services." Claims 4 and 32 specify that a plurality of roles are "combined into role-groups that may be assigned to one or more hosts." Claims 5 and 33 specify that a plurality of hosts are "combined into a host-group that may be assigned a role or a role-group." Reid et al. and Grennan, alone or in combination, do not disclose or suggest the idea of "roles," as used in the present invention.

In view of the foregoing, the invention, as claimed in Claims 1 through 8, 29 through 35 and 38 cannot be said to be either taught or suggested by Reid et al. and Grennan, alone or in combination. Accordingly, applicants respectfully request that the rejection of claim 1 through 8, 29 through 35 and 38 under 35 U.S.C. §§102 or 103 be withdrawn.

All of the pending claims, i.e., claims 1 through 8, 29 through 35 and 38, are in condition for allowance and such favorable action is earnestly solicited.

If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this application, the Examiner is invited to contact the undersigned at the telephone number indicated below.

The Examiner's attention to this matter is appreciated.

Respectfully,

Kevin M. Mason

Date: April 25, 2002

Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06430
(203) 255-6560

VERSION MARKED TO SHOW ALL CHANGES

IN THE CLAIMS:

Please amend the claims as follows:

Please cancel claims 9-28, 36 and 37, without prejudice.

1. (Amended) A method for generating a configuration file for at least one firewall in a network, said network including a plurality of hosts, said method comprising the steps of:

receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network;

receiving an assignment of said roles to said hosts in said network; and

generating rules for said hosts based on said assigned roles, said rules determining whether a packet is passed to a destination host.

2. The method of claim 1, wherein a configuration file is generated for a plurality of firewalls in said network.

3. The method of claim 1, wherein a security policy for said network is expressed in terms of said roles defining network capabilities of sending and receiving services.

4. The method of claim 1, wherein a plurality of said roles are combined into role-groups that may be assigned to one or more hosts.

5. The method of claim 1, wherein a plurality of said hosts are combined into a host-group that may be assigned a role or a role-group.

6. The method of claim 1, further comprising the step of providing a visual representation of the structure of said hosts in said network.

7. The method of claim 1, further comprising the step of providing a visual representation of a set of rules in said configuration file.

8. The method of claim 1, wherein said generating step is performed by a vendor-specific compiler that produces a vendor-specific firewall configuration file.

32 (Amended) A method of generating a security policy for a network, said network including a plurality of hosts, said method comprising the steps of:

receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network;

receiving an assignment of said roles to said hosts in said network; and

generating said security policy from said received definitions and assignments.

33 The method of claim 29, further comprising the step of translating said security policy into at least one configuration file for a firewall on said network.

34 The method of claim 30, wherein said configuration files are generated for a plurality of firewalls in said network.

35 The method of claim 29, wherein a plurality of said roles are combined into a role-group that may be assigned to a host.

36 The method of claim 29, wherein a plurality of said hosts are combined into a host-group that may be assigned a role or role-groups.

37 The method of claim 29, further comprising the step of providing a visual representation of the structure of said hosts in said network.

38 (Amended) A compiler for generating a configuration file for a firewall in a network, said network including a plurality of hosts, comprising:

a memory for storing computer-readable code; and

a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network;

receive an assignment of said roles to said hosts in said network; and

generate rules for said hosts based on said assigned roles, said rules determining whether a packet is passed to a destination host.

38. (Amended) A system for generating a security policy for a network, said network including a plurality of hosts, said system comprising:

a memory for storing computer-readable code; and

a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network;

receive an assignment of roles to said hosts in said network; and

generate said security policy from said received definitions and assignments.